In sections 10-12, 14 and 15 of the "Response to Amendment" section of the Action, the Examiner provides a number of statements in response to Applicant's arguments set forth in the response dated October 14, 2004. However, it is respectfully submitted that these statements do not serve to remedy the deficiencies pointed out in Applicant's prior response, for the following reasons:

Independent Claims 1, 5 and 7

Starting on page 7 of the response, Applicant pointed out that the Kakiuchi et al. patent fails to teach or suggest, among other things, the "first controller which operates to determine whether data on output request passes the driver software, in sending data to the output device." Specifically, in lines 9-16, Applicant argued:

> [T]he portions of Kakiuchi et al. relied upon in the Office Action (i.e., column 4, lines 20-31, column 9, lines 54-65, column 10, lines 26-33 and column 12, lines 36-49) do not mention any *determination* being made by a controller concerning whether data on output request passes driver software as claimed. The cited portions, which describe embodiments shown in Figures 1 and 4 of Kakiuchi et al., in fact, appear to describe a system in which the data always passes driver software (i.e., "printer driver 103") when sent to an output device (i.e., "printer 902") on an output request."

In section 11, the Examiner disagrees with this analysis, and with reference to column 3, lines 23-44 of Kakiuchi et al., the Examiner states, "Kakiuchi discloses a controller that includes an examination means that determines whether data passes the driver software by determining whether data is sent to the output device" (emphasis added). The Examiner goes on to state that the output device is the printer. It is respectfully submitted, however, that column 3, lines 23-67 of the Kakiuchi et al. patent relied upon by the Examiner do not relate to any determination made by a controller as to whether data on output request passes driver software for controlling the output device. Rather, the cited parts of the Kakiuchi et al. patent describe a controller, which includes:

1. A first examination means for examining whether received input data includes data that can correspond to data as an object of a prescribed examination;

2. A second examination means for examining in detail data which can correspond to the data as an object of examination to determine whether it is the object data when the first examination means detects that the input data includes the data which can correspond to the data as an object of a prescribed examination, and

3. Data processing means for permitting printing of the input data when the first examination means detects that the input data does not include the data which can correspond to the data as an object of a prescribed examination or the second examination means detects that the data which can correspond to the data as an object of examination is not the object data.

As can be seen from the above, items 1 and 2 of the Kakiuchi et al. printer controller define two stages of examination that determine whether data to be printed is an object of examination. The data processing means (item 3 above) controls the printer in accordance with the examination result of item 2 and/or item 1. However, there is simply no mention, nor is there any suggestion in Kakiuchi et al., that a printer controller operates *to determine whether data on output request passes the driver software*. Moreover, because data to be output by the printer of Kakiuchi et al. always passes the printer driver by way of an application program (i.e., item 102) that provides a command to the driver software (see, column 11, lines 24-25, column 12, lines 31-32, and command C1 and drivers 101, 103 depicted in Figures 1 and 4), there would be no apparent reason for the printer controller to determine whether or not data on output request passes the driver software.

Even if one were to assume, *arguendo*, that some determination is made as to whether data is sent to the output device, as alleged by the Examiner, the Kakiuchi et al. printer controller appears to always assume that received data has been sent by the printer driver. See, for instance, the data path from the printer driver 101 for the ink jet printer embodiment of Figure 1, and the printer driver 103 for the laser printer embodiment of Figure 4, to respective printer controllers 203, 203a.

With respect to the Nagashima patent, which is relied upon for purportedly teaching the next recited feature of "a second controller for prohibiting data from being sent to the output device for output request on which data bypasses the driver software," the Examiner states,

> Nagashima discloses an image processing circuit that includes a forgery preventing mode, that determines if the copying is a forgery copying is prevented for performing. This forgery prevention mode is a part of the controller (see column 3, lines 50-65). (See, page 5, section 12, lines 3-6.)

It is respectfully submitted that this statement by the Examiner does not address the points of distinction raised in Applicant's response. Furthermore, it does it provide any substantive information from the Nagashima et al. patent of a second controller that operates to prohibit data from being sent to an output device for output request *on which data bypasses the driver software*, as claimed.

As Applicant pointed out starting at the last two lines of page 7 of the October 14, 2004 response, the Nagashima et al. patent does not mention anything whatsoever about driver software in connection with data being output from the controller 4 because Nagashima et al. is not concerned with the particulars of the host computer connected to the external controller 4 (see, for example, column 4, lines 3-5 and column 5, lines 23-25). In fact, the only mention of a "driver" *per se* in Nagashima et al. is one that drives a semiconductor laser (column 10, lines 39-40 and item 306 shown in Figure 10). According to Nagashima et al., the controller 4 and color copying apparatus operate under a common encryption specification so that output data sent to the printer 13 will be abnormal when an encryption information signal of another specification is input to disable encryption (see column 5, lines 4-7). It is respectfully submitted, however, that such common encryption specification would not have taught or suggested whether data is sent "directly" to an output device *bypassing any driver software*, as is alleged by the Examiner.

Even if one were to consider, for the sake of argument, that one of ordinary skill in the art would have been motivated to somehow modify the Kakuichi et al. system to include the external controller of Nagashima et al., such a combination would not have taught or suggested the claimed combination including a first controller that operates to determine whether data on output request passes driver software, and a second controller for prohibiting data from being sent to the output device for output request on which data bypasses the driver software. To the contrary, it would appear that such proposed modification of Kakiuchi et al. would perhaps have suggested a system in which output data sent to an output device *always* passes a printer driver.

MPEP § 2143 instructs that one of the basic requirements that must be adhered to establish a *prima facie* case of obviousness is that the references must teach or suggest all the claim limitations. As pointed out above, the Kakiuchi and Nagashima patents fail to teach or suggest all the limitations set forth in claim 1, regardless of whether these documents are considered individually or in the proposed combination. Accordingly, independent claim 1 is allowable.

Similar distinctions are recited in independent claims 5 and 7. For instance, each of claims 5 and 7 recite *inter alia* acts of determining whether data on output request passes driver software incorporated in the data processing device for controlling an output device, in sending data to the output device from the data processing device, and prohibiting data from being sent to the output device for the request on which data bypasses the driver software. For reasons similar to those above, these features are not taught or suggested by the proposed combination of the Kakiuchi et al. and Nagashima patents. Hence, claims 5 and 7 also are patentable.

Independent Claims 2, 6 and 8

In connection with independent claim 2, section 14 of the Action includes the following statements:

> The Applicant states that Nagashima et al. does not disclose an encryptor for encrypting data passing the driver software, but not for encrypting data sent to the output device that bypasses the driver software. Nagashima et al. discloses that encryption/decryption is performed in the controller (see col. 3, lines 51-55). Nagashima et al. does not disclose that encryption is performed all the time. Nagashima discloses that a determining circuit executes forgery determination, it does not disclose that in the forgery determination encryption is done (see col. 4, lines 54-63).

It is respectfully submitted, however, that these statements by the Examiner do not address the fact that the cited parts of Nagashima et al. do not even mention driver software as claimed, much less claimed encryptor and decryptor operation in connection with data passing and bypassing the driver software. In the statements of the rejection, the Examiner nevertheless continues to allege that because

Nagashima discloses a controller (i.e., "external controller 4") sending data to the output device directly, the data bypasses driver software. (See, lines 10-14 of section 3.) However, this allegation is not substantiated by evidence existing in the Nagashima et al. patent. Furthermore, Applicant's arguments pointing out this fact remain unanswered. (See page 9 of the October 14, 2004 response.) For instance, Applicant argued that the Nagashima et al. patent is not concerned with the details of an external image processing apparatus (see column 3, lines 6-9 of Nagashima et al.), such as a host computer (column 4, lines 3-5), and thus Nagashima et al. does not discuss any details of driver software, such as whether data passes and bypasses the driver software, as claimed.

To the extent that section 5, line 1 of the Office Action appears to also rely on the Kakiuchi et al. patent for teaching driver software (see, page 3, lines 1-4 of section 5), Applicant's previous response pointed out that the cited parts of Kakiuchi et al. describe two separate embodiments in which data to be output to the printer *always* passes the driver software. Kakiuchi et al. also does not mention or suggest data provided to the output device as data that has bypassed driver software, as claimed.

Hence, as neither Kakiuchi et al. nor Nagashima et al. mention or even hint at data sent to the output device *bypassing* driver software, these documents cannot suggest the claimed "encryptor for encrypting data passing the driver software, provided on the data processing device, but not for encrypting data sent to the output device that bypasses said driver software; and a decryptor for decrypting data encrypted by the encryptor and output data that bypasses said driver software, provided on the output device," as set forth in independent claim 2. Accordingly, the rejection is improper for these reasons alone.

Similar distinctions are brought out in claims 6 and 8 with respect to processes performed by an output system and a program product. For instance, claim 6 is directed to a method in which data is encrypted for data passing the driver software included in the data processing device, on the data processing device side, but not data that bypasses said driver software when sent to the output device is not encrypted. Claim 8 recites the steps of "encrypting output data from an application program run on the data processing device that passes driver software stored in the data processing device for controlling the output device, and outputting the encrypted data to the output device, wherein said step of encrypting is not performed for data output to the output device that bypasses the driver software." As pointed out above, the Kakiuchi et al. and Nagashima et al. patents do not teach or suggest selectively performing encryption operations based on whether output either data passes or bypasses driver software. As such, there is no teaching or suggestion of whether to perform encryption on these data as recited in each of claims 6 and 8.

Moreover, claim 6 recites that if data is present at the output device, which had bypassed the driver software and had not been encrypted, it is decrypted. This feature also is not taught or suggested in the Nagashima et al. patent. Additionally, the Office Action fails to address this claimed feature in any way.

As noted above, a *prima facie* case of obviousness requires the Examiner to show that all claim limitations are taught or suggested in the cited documents. However, none of the cited patents, considered individually or in combination, teach or suggest the encryptor and decryptor of claim 2, the encrypting process of claim 8 and the encrypting/decrypting processes of claim 6, all of which involve consideration of whether data either passes or bypasses driver software. Thus, claims 2, 6 and 8 are allowable.

Independent Claim 10

In response to undersigned's request that the Examiner point out the specific lines in the cited parts of the Kakiuchi et al. patent that allegedly teach a step of "installing a program for prohibiting data on output request from being sent to the output device, for request on which data bypasses the driver software" as recited in claim 10, the Examiner refers to lines 60-62 of column 7. (See section 15 of the Action.) However, merely installing driver software on a hard disc as described in this cited part of Kakiuchi et al. does not relate to the claimed step of installing a program that is operative to prohibit data on an output request from being sent to an output device, *for request on which data bypasses the driver software*. As pointed out above, none of the parts Kakiuchi et al. and Nagashima et al. relied upon teaches or suggests consideration of whether data on output request has bypassed driver software. As the Examiner has been asked to show where such features are described in the applied documents, and she has failed to provide any factually based evidence to support her allegations, the rejection is clearly improper. Therefore, the rejection should be withdrawn.

Conclusion

Based on the foregoing, withdrawal of the rejection of the claims is believed warranted. Should residual issues exist, the Examiner is invited to contact the undersigned at the number listed below to resolve any such issues and allow the application without further delay.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

Date: April 14, 2005

By: John Guay
John F. Guay
Registration No. 47,248

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620